

Najnovšie post-kvantové štandardy v kryptografii

Vladyslav Lanovyi

Obsah

1	Chronológia vývoja kryptografických štandardov	5
1.1	Symetrické štandardy	5
1.1.1	DES (Data Encryption Standard)	5
1.1.2	AES (Advanced Encryption Standard)	5
1.2	Štandardizácia verejno-klúčovej kryptografie	5
1.2.1	DSS (Digital Signature Standard)	5
1.3	Hašovacie štandardy	5
1.3.1	SHS (Secure Hash Standards)	5
2	Kvantova a post-quantova kryptografia	6
2.1	Kvantova kryptografia	6
2.2	Postkvantova kryptografia	6
3	NIST štandarty pre post-quantovú kryptografiu	7
3.1	FIPS-203 (CRYSTALS-Kyber)	7
3.1.1	Zakladne pojmy a opis	7
3.2	FIPS-204 (CRYSTALS-Dilithium)	7
3.2.1	Zakladne pojmy a opis	7
3.3	FIPS-205 (SPINCS+)	7
3.3.1	Zakladne pojmy a opis	7
4	Experimentálna časť	8
5	Záver	9

Zoznam skratiek

AES - Advanced Encryption Standard

DES - Data Encryption Standard

RSA - Rivest-Shamir-Adleman

ECC - Elliptic Curve Cryptography

ECDSA - Elliptic Curve Digital Signature Algorithm

SHA - Secure Hash Algorithm

NTT - Number Theoric Transform

Úvod

1 Chronológia vývoja kryptografických štandardov

1.1 Symetrické štandardy

1.1.1 DES (Data Encryption Standard)

1.1.2 AES (Advanced Encryption Standard)

1.2 Štandardizácia verejno-klúčovej kryptografie

1.2.1 DSS (Digital Signature Standard)

1.3 Hašovacie štandardy

1.3.1 SHS (Secure Hash Standards)

2 Kvantova a post-quantova kryptografia

2.1 Kvantova kryptografia

2.2 Postkvantova kryptografia

3 NIST štandardy pre post-kvantovú krypto- grafiu

3.1 FIPS-203 (CRYSTALS-Kyber)

3.1.1 Zakladne pojmy a opis

3.2 FIPS-204 (CRYSTALS-Dilithium)

3.2.1 Zakladne pojmy a opis

3.3 FIPS-205 (SPINCS+)

3.3.1 Zakladne pojmy a opis

4 Experimentálna časť

5 Závěr

Literatúra